# POLICY
# FOR THE PROTECTION OF PERSONAL DATA OF INSURANCE COMPANY EUROINS AD

## INFORMATION CARD

| | |
|---|---|
| **Date of adoption of the document:**<br>**Date of entry into force:** | **30.01.2020**<br>**30.01.2020** |
| **Version of the document:**<br>**Effective from:** | **2.2**<br>**10.12.2025** |
| **Structure, document publisher:** | **Methodology and Business Processes Department** |
| **Document validity period:** | **Indefinite** |
| **Approved by/on:**<br>**Amended by/on:** | **Management Board/30.01.2020**<br>**Board of Directors/18.12.2020**<br>**Board of Directors/10.12.2025** |

## CONTENTS:

## CHAPTER I. GENERAL PROVISIONS

**Art.1**.(1) Euroins Insurance Company AD (Euroins, the Company, the Controller) is a legal entity with its registered office and address of management at: 1592 Sofia, Iskar District, 43 "Hristofor Kolumb" Blvd. and whose main activity is insurance and insurance services.

(2) The Company is a personal data controller within the meaning of Article 4(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR).

(3) The Company, as a personal data controller, complies with, discloses, and provides information to data subjects within the meaning of Articles 13 and 14 of the GDPR through a Privacy Notice in connection with the provision of insurance services, Privacy Notice for employees and persons employed under civil law contracts, a Privacy Notice regarding personal data processed by Euroins Insurance Company AD in its capacity as a personal data controller in the selection of personnel, and Rules for providing information on the exercise of the rights of personal data subjects.

(4) As a personal data controller, the Company determines:

1. the type of data processed, in accordance with the intended purposes;
2. the purpose and means of processing;
3. measures to ensure the security of personal data, in compliance with the requirements of the GDPR, the Personal Data Protection Act, and other normative acts.

**Art.2**.(1) This Personal Data Protection Policy of Euroins (the Policy) aims to regulate:

1. the keeping, maintenance, and protection of personal data registers (personal data processed by the Company);
2. the obligations of persons authorized to process personal data and their responsibility;
3. the necessary technical and organizational measures to protect personal data from unlawful processing (unlawful destruction, loss, alteration, unauthorized disclosure or access to personal data by third parties, as well as from all other unlawful forms of personal data processing).

(2) The policy applies to personal data processed within the Company.

(3) The Company processes personal data in compliance with the following basic principles (pursuant to Article 5 of the GDPR):

1. lawfulness, fairness, and transparency;
2. purpose limitation;
3. minimization of data;
4. accuracy;
5. storage limitation;
6. integrity and confidentiality.

(4) The company is responsible for being able to prove compliance with the principles related to the processing of personal data at any time (principle of accountability).

(5) The company processes personal data independently, by written assignment to a personal data processor or as a joint controller (pursuant to Article 26 of the GDPR).

(6) Any person acting under the direction of the Company who has access to personal data shall process such data only on the instructions of the Controller – Article 29 of the GDPR. Such persons are:

1. employees of Euroins whose job duties or specific assigned tasks require the processing of personal data. These persons are part of the structure of the Controller;
2. other persons (e.g. under a civil contract) who have access to personal data in order to perform the tasks or activities assigned to them. These persons are outside the structure of the Controller.

## CHAPTER II. PURPOSE AND MAINTENANCE OF REGISTERS

**Art.3**.(1) The company structures, organizes, maintains, and updates the personal data registers, independently determining the purposes and means of data processing.

(2) The registers shall be maintained in written form and in electronic format. The data carriers shall be stored in designated premises with regulated access.

**Art.4**.(1) Paper data carriers containing personal data shall be stored in folders (files) in a manner that prevents any breach of their integrity or loss of information protected by law.

(2) Access to the relevant files shall be restricted to authorized employees of the Company, in accordance with their job and functional characteristics and direct instructions from the representatives of Euroins. The possibility of granting another person access to personal data during its processing is limited and expressly regulated in this Policy, another written document of the Company, or in the regulatory framework.

**Art.5**.(1) The processing of personal data in electronic format is carried out only in the corporate network, which is not connected to the public network, and the rights to access and process personal data in the systems are determined and granted in compliance with the official commitments and in accordance with the terms and conditions set out in the Access Management Rules. When working with data, software products for data processing are used that are adapted to the specific needs of the Company.

(2) Access to operating systems where personal data is processed is restricted to authorized persons with a username and password for authentication. The protection of electronic data from unauthorized access, damage, loss, or destruction is ensured by maintaining firewalls, antivirus programs, updating operating systems, periodically archiving data, periodically changing passwords, VPN, as well as by maintaining the information on paper.

## CHAPTER III. PERSONAL DATA STORED IN REGISTERS

**Art.6**.(1) The human resources register collects and stores the personal data of job applicants, persons employed under labor or civil law relationships and related to these persons, third parties, when such data is required for the application of the legislation (family members, persons in an economic or other regulatory relationship) in connection with the administration of processes related to the Company's obligations under labor, tax, and social security legislation and special legislation relevant to its activities, for the purpose of:

1. staff selection;
2. individualisation of the parties in labour and civil legal relations;
3. compliance with the regulatory requirements of the Labor Code, the Social Security Code, the Health Insurance Act, the Personal Income Tax Act, the Accounting Act, the Obligations and Contracts Act, the Insurance Code, and others;
4. for all activities related to the existence, amendment, and termination of labor and civil legal relationships — for the preparation of any documents of persons in this regard (contracts, additional agreements, documents certifying work experience, official notes, references, certificates, and other similar documents), procedures related to qualification and reliability requirements, and procedures related to requirements for employers to ensure healthy and safe working conditions, and others;
5. correspondence with supervisory authorities and other regulations specific to the activity;
6. establishing contact with the person by telephone, sending correspondence to a physical or electronic address relating to the administration and performance of employment or civil contracts to which the data subject is a party;
7. for keeping accounting records, for the remuneration of the above-mentioned persons under employment and civil contracts;
8. others as specified in the Privacy Notice for employees and persons employed under civil law and the Privacy Notice regarding personal data processed by Euroins in its capacity as a personal data controller in the selection of personnel.

(2) The personal data of the Company's employees is organized in personal employment files and stored in a filing cabinet. They are located in a specially equipped room intended for the work of the authorized employee(s) involved in human resources management activities.

(3) Access to the information in the personnel files stored by automated means is granted to the authorized employee(s) referred to in paragraph 2, second sentence, by means of a password to open these files. The possibility of granting another person access to personal data during its processing is limited and expressly regulated in this Policy and the relevant internal rules of the Company, insofar as it does not arise from the applicable legislation.

(4) The following categories and types of data are processed in the register:

1. Identification information (physical identity) – full name, personal identification number, identity card number, date and place of issue, place of birth.

2. Contact information/location information – contact telephone numbers, email address, permanent/current address or correspondence address.
3. Economic identity – bank account details for payment of remuneration, details of financial status and economic ties, in accordance with the Insurance Code.
4. Social identity – education and work experience, documents certifying education, qualifications, and legal capacity, where required for the position for which the person is applying, etc., documents certifying employment and professional biography, documents certifying family ties and marital status (marriage certificate, child birth certificate, declarations of affiliation), data related to convictions and violations – criminal record certificate, when required for the position, declarations of qualification and reliability.
5. Special categories of personal data (health identity) – data on the person's health status contained in a medical certificate for starting work, expert opinions from medical examination authorities in connection with the provision of documents for temporary incapacity for work and permanent reduced working capacity, data on religious affiliation other than Orthodox Christianity, when declared by the person for the exercise of the rights under Article 173 of the Labor Code.

(5) The data for this register shall be collected upon the commencement/assignment of work under an employment or civil law relationship of a given person in compliance with a regulatory obligation – the provisions of the Labor Code, the Social Security Code, the Health Insurance Act, the Personal Income Tax Act, the Accounting Act, the Obligations and Contracts Act, the Insurance Code, and others in one of the following ways:
1. Oral interview with the person (upon entry into service or in the course of employment).
2. On paper – written documents – applications, requests for employment/performance of work under an employment or civil law relationship and the attached documents, for amendment or termination of these relationships, on current issues in the course of employment, submitted by the person.
3. From external sources (from judicial, financial, insurance, tax, and other institutions in compliance with regulatory requirements).
4. In all cases where it is necessary on the basis of a regulatory obligation, persons whose data must be processed in the register shall submit the necessary personal data to the Controller or to the authorized employee, respectively.

(6) The employee from the Human Resources Department shall be obliged to provide the data subject with the information under Article 13 of the GDPR in accordance with the template no later than the moment of receiving the data from him/her.

(7) In certain cases, limited access to personal data from this register may be granted to: members of the Board of Directors of Euroins, the chief accountant, as well as persons performing technical accounting operations in the preparation of payment documents related to bank transfers of remuneration, as well as other employees of the Company who need to process personal data in order to perform their duties in accordance with their job description, for example, but not limited to, legal advisors.

(8) The authorized employee under paragraph 2, second sentence, shall provide access to the information stored by him/her in compliance with the requirements of this Policy, and in cases not covered by it, upon written instruction from a representative of the Company.

(9) Personal data collected during the recruitment process shall be processed and stored in accordance with the Privacy Notice regarding personal data processed by Euroins in its capacity as a personal data controller during the recruitment process.

**Art.7**.(1) The register of the Company's customers – users of insurance services and intermediaries – collects and stores personal data of counterparties, intermediaries, and users of insurance services for the purposes of:
1. insurance purposes – activities related to providing insurance coverage for risks under a contract, consisting of collecting and spending funds intended for the payment of compensation and other monetary amounts upon the occurrence of events or the fulfillment of conditions provided for in a contract or by law, as well as activities directly related thereto, including:

a) insurance risk assessment/tariff setting;
b) determination of the insurance premium;
c) determination of an insured event;
d) determining the amount of damage caused;

e) transferring all or part of the insurance risks covered by an insurer to a reinsurer or another insurer;
f) other
2. individualisation of persons for the relevant type of insurance;
3. compliance with the regulatory requirements under the Insurance Code and others;
4. for all activities related to the preparation of any documents and reports for persons (certificates, attestations, assurances, and the like);
5. establishing contact with the person by telephone, sending correspondence relating to the performance of the relevant contract;
6. others as specified in the Privacy Notice in connection with the provision of insurance services.

(2) Employees who are directly involved in the activities of concluding and administering insurance and brokerage contracts are obliged to make available to data subjects the information under Articles 13 and 14 of the GDPR in the form of the Privacy Notice in connection with the provision of insurance services, as approved and published on the Company's official website.

(3) Paper carriers of personal data shall be stored in document pockets, folders, binders, cabinets, metal safes, and other similar tools for organizing, arranging, and storing documentation. In the office premises where the data is processed, such as parts of buildings or separate wings of floors, physical access is controlled and intended for the work of authorized employees of the Company who are required to process personal data carriers and other information protected by law, in accordance with their job description.

(4) When keeping the register on electronic media, personal data shall be entered and processed in corporate networks and software programs with access control.

(5) The following types of data shall be maintained in the register:

1. Identification information (physical identity) – full name, personal identification number, data from identity document.
2. Contact information/location information – email, address, and telephone number.
3. Economic identity – bank account number, property status data (owned property, such as motor vehicle data, real estate), payment history.
4. Social identity – employment history, professional experience, occupation, remuneration.
5. Special categories of personal data (health identity) – information about the health status of insurance service users (diagnosis, medical records, other medical documents for examinations, tests, or other interventions).

(6) The personal data in the register under Article 7 shall be collected upon conclusion of the relevant type of contract, submission of a claim/registration of damage, complaint, etc., by the natural persons to whom the data relate (the insured persons, respectively the insurers and/or the injured persons, respectively their proxies), state authorities and third parties, in accordance with the Insurance Code and from public registers.

**Art.8**.(1) The register concerning the Company's records and archives collects and stores personal data on various categories of natural persons – users of insurance services, intermediaries, providers, legal representatives and proxies, including data provided in connection with the establishment and exercise of legal claims before judicial and extrajudicial authorities, and data processed through inquiries from regulatory and supervisory authorities. Also, reports under the Law on the Protection of Persons Reporting Violations or Publicly Disclosing Information about Violations (the personal data of whistleblowers, persons assisting them, and persons related to them, including affected persons who fall within the scope of the Law on the Protection of Persons Reporting Violations or Publicly Disclosing Information about Violations).

(2) The data in the register under Article 8, paragraph 1 shall be collected and processed for the purpose of managing the filing and archiving of paper documents in compliance with the Company's internal rules, procedures, instructions, and guidelines.

(3) The archiving and storage of documents shall be carried out in accordance with the Rules for Archival Activities, the Instructions for the Application of the Nomenclature of Cases, and the Nomenclature of Cases with Storage Periods.

(4) The following categories of personal data are processed in the register under Article 8, paragraph 1:

1. Identification information (physical identity) – names, personal identification number/foreign national identification number, identity document data.

2. Contact information/location information – email, address, and telephone number.
3. Other data – provided at the discretion of the natural person who is the author of the initiating document filed in the Company's filing system.

**Art.9**.(1) The Company may process personal data in whole or in part by automatic means in personal data registers for purposes arising from the legitimate interests of the Controller or a third party (such as video surveillance, access cards, and others) in the context of:
1. physical security management;
2. property security;
3. access control;
4. monitoring of employees for the purposes of performing their duties and using resources and information;
5. information technology security;
6. network security;
7. improvement of customer service.

(2) The Company processes personal data of persons employed under employment and other legal relationships and of third parties:
1. passing through a secure perimeter;
2. calling the telephone exchange of Euroins;
3. visiting the Company's buildings/offices;
4. accessing information resources on legitimate grounds or using resources for which security and surveillance systems are used.

(3) The processing is carried out through access cards, video surveillance systems, GPS systems on company cars, and monitoring of company information resources.

(4) The data is collected in the course of implementing the relevant technical and organizational protection measures to prevent unauthorized access to buildings, premises, facilities, and systems where personal data is processed in connection with the activities of Euroins.

(5) The following categories of personal data are processed in the register under Article 9:
1. Identification information (physical identity) – employee names, employee card numbers, work email addresses, positions, logos, photos or videos, including persons falling within the scope, recordings of telephone conversations made when calling to and from the Company's telephone exchange.
2. Location information – geographical location;
3. Online identifiers – passwords, username, IP address of the device used, device data when using a VPN.

## CHAPTER IV. IMPACT ASSESSMENT AND TECHNICAL AND ORGANIZATIONAL MEASURES FOR THE PROTECTION OF PERSONAL DATA

**Art.10**.(1) Upon joining the Company, and subsequently on a regular basis, but no less than once a year, employees shall be familiarized with the requirements of the applicable legislation governing the protection of personal data, as well as with this Policy.

(2) Employees of the Company who, due to the nature of their work and/or position, are assigned to process personal data, shall be obliged to comply with the legislation governing the protection of personal data in their actions. They shall be liable under Bulgarian law for any failure to comply with this obligation.

**Art.11**.(1) The Company shall designate or appoint a data protection officer (DPO), of whom it shall duly notify the supervisory authority for personal data protection and the data subjects. This person can be contacted via email at dpo@euroins.com or office@euroins.com.

(2) Functions of the DPO:
1. Participates in an appropriate and timely manner in the resolution of all issues related to personal data protection, including, but not limited to, when decisions are made that affect data processing and protection (adoption and amendment of new internal policies, rules, and procedures, introduction of new software and business products), as well as when a data breach or other incident is detected.
2. Acts as a contact person for the supervisory authority and data subjects, who may contact the DPO on all matters related to the processing of their personal data and the exercise of their rights under the GDPR.
3. Informs and advises the Controller and employees who process personal data on their obligations to comply with data protection legislation, the Company's internal rules, participates in activities to raise

staff awareness, including organizing and conducting training on topics related to data processing and security protection.
4. Monitors compliance with data protection legislation and the Company's internal rules by collecting information to determine processing activities, analyzing and verifying their implementation, and making recommendations to the Controller.
5. Expresses an opinion on the need to carry out a data protection impact assessment (DPIA) for a specific type of processing, what methodology to use to perform it, what safeguards to apply to reduce the risks to the rights and interests of data subjects, whether the DPIA has been performed correctly, and whether the conclusions lead to the need for prior consultation with the supervisory authority.
6. Keeps a register of processing activities in accordance with Article 30 of the GDPR, an operational register of requests for the exercise of rights, and a register of data security breaches.
7. Performs other activities in accordance with his/her job description.
(3) The DPO is independent and the Controller provides him/her with technical, organizational, training, financial, and any other assistance, as well as access to the relevant registers and operations, to the extent necessary in connection with the performance of his/her duties.
(4) The DPO shall observe confidentiality and secrecy in the performance of his/her tasks arising from this Policy and the applicable legislation.
**Art.12**. The Register of Processing Activities pursuant to Art. 30 of the GDPR shall describe the processing of personal data in the Company's data registers.
**Art.13**.(1) Personal data in the maintained registers shall be stored and protected from accidental or unlawful destruction, accidental loss, unauthorized access, alteration, or dissemination, as well as from other unlawful forms of processing through a system of technical and organizational measures.
(2) The protection of personal data is:
1. physical;
2. personal;
3. documentary;
4. protection of automated information systems and/or networks;
5. cryptographic protection.
(3) Measures for the protection of personal data shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, including, where appropriate, the measures referred to in Article 32 of the GDPR.
(4) The technical and organizational measures that the Company applies to individual registers and processing activities shall be entered in the Register of Processing Activities pursuant to Article 30 of the GDPR. The measures shall be updated and subject to periodic review in the event of changes in the purposes, means, or grounds for processing, as well as at the proposal of the units (departments/directorates) involved in the personal data processing processes, recommendations from audits and inspections, or at the proposal of the DPO.
(5) Physical protection measures include rules, procedures, and orders of the Company's Management Board to prevent unauthorized access to buildings, premises, and facilities where personal data is processed, such as: controlled access, movement, and exit from work premises; storage of keys to premises, safes, cabinets, and other facilities used to store information containing personal data, fire extinguishing systems, regulated visiting hours, and others.
(6) Personal protection includes a system of organizational measures ensuring an appropriate level of knowledge of the regulatory framework in the field of personal data protection, obligations for non-disclosure of critical information among staff and outside the Company, training, training of employees in crisis response, including events that threaten data security.
(7) Documentary protection is a system of organizational measures that are expressed in the regulation of activities related to the processing of personal data through policies, procedures, and rules, as well as the maintenance of activity logs, Operational register of requests for the exercise of rights, procedures for storage, access, and destruction of data carriers, determination of storage periods.
(8) The company applies a system of technical and organizational measures when processing data through information systems in order to protect against unlawful forms of personal data processing, which ensures a clear distribution of roles and responsibilities, identification and authentication, session and remote access controls, virus protection, and maintenance of backup copies for recovery. The

implementation of the protection measures is ensured through the Information Security Policy and a system of procedures and rules for managing access to information systems, changes, configuration of the antivirus system, and others. Employees of the Information Technology and Digitalization Department perform ongoing analysis of the ability of the network and information systems to withstand a high level of accidental events, unlawful or malicious actions that could have a significant impact on the integrity, availability, and confidentiality of the data processed, stored, and transmitted within the Company and, if necessary, propose changes commensurate with the levels of risk.

(9) Cryptographic protection is a system of technical and organizational measures applied to protect personal data from unauthorized access during transmission, distribution, or provision. The main measures of cryptographic protection are:

1. the standard cryptographic capabilities of operating systems;
2. the standard cryptographic capabilities of database management systems;
3. standard cryptographic capabilities of communication equipment;
4. systems for the distribution and management of cryptographic keys;
5. legally defined electronic signature systems.

**Art.14**.(1) A DPIA is a process that aims to describe the processing of personal data, assess its necessity and proportionality, and help manage the risks to the rights and freedoms of individuals by assessing them and determining measures to address those risks.

(2) A DPIA is mandatory for an operation or set of operations where the processing is likely to result in a high risk to the rights and freedoms of natural persons, as well as for operations included in the list of the supervisory authority under Article 35(4) of the GDPR. The controller shall justify and document the reasons for its decision whether to carry out a DPIA, including by requesting the opinion of the DPO. Where the processing is carried out wholly or partly by a processor, the processor shall assist the controller in performing the DPIA in accordance with the requirements of the GDPR, taking into account the nature of the processing and the information to which it has access. The role and responsibilities of the personal data processor with regard to the DPIA shall be specified in the contract concluded.

(3) The units (departments/directorates) responsible for personal data processing processes shall determine the purposes and means of processing and/or risk assessment, and the DPO may propose that a DPIA be carried out. They provide the necessary information for the DPIA and participate in the process of documenting and validating it.

(4) When performing a DPIA, an appropriate methodology is used, the content of which complies with the published guidelines, recommendations, and best practices of the competent data protection authorities (supervisory authority and European Data Protection Board, respectively Working Party on the Protection of Individuals with regard to the Processing of Personal Data under Article 29).

**Art.15**.(1) Personal data shall be stored until the purposes for which it was collected have been achieved and in accordance with the time limits set for storage on the relevant medium.

(2) The storage and destruction of personal data carriers shall be carried out in accordance with the Company's approved Rules for Archival Activities; Nomenclature of Files with Storage Periods; Procedure for Transferring Documents to the Archive; Procedure for Destruction of Documents.

## CHAPTER V. RIGHTS OF DATA SUBJECTS AND THE PROCEDURE FOR EXERCISING THEM

**Art.16**.(1) Data subjects may exercise their rights under Articles 15-22 of the GDPR by submitting a written request to the Controller. The request may be submitted:

1. electronically, signed with an advanced electronic signature based on a qualified certificate for electronic signatures, or a qualified electronic signature, as specified in the Rules for providing information for the exercise of the rights of personal data subjects;
2. in person at the office of Euroins by the data subject. If the request is submitted by an authorized representative, the original power of attorney shall be presented for verification;
3. by mail to the address of the Company's Central Administration (43 Hristofor Kolumb Blvd., Sofia);
4. and is free of charge.

(2) Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Controller may charge a reasonable fee or refuse to act on the request.

**Art.17**.(1) The application for exercising personal data rights should contain the following information:

1. Identification of the person – full name and additional identification data such as personal identification number, or foreigner identification number, or other similar identifier, or policy number, or customer number.
2. Accurate and specific description of the request.
3. Preferred form of provision (sending) of the information.
4. Signature, date of submission of the application, and correspondence address.

(2) The application shall be registered in the Company's general incoming register and in the Operational Register of requests for the exercise of data subjects' rights, maintained by the DPO.

**Art.18**. Access to the person's data shall be provided in the form of:
1. verbal inquiry;
2. written inquiry;
3. review of the data by the person themselves or their representative;
4. provision of a copy of the requested information.

**Art.19**.(1) Upon receipt of a request from a data subject under Art. 16, the application shall be submitted to the DPO for consideration and preparation of a reasoned draft decision.

(2) The units in which personal data are processed shall cooperate in the course of the examination of the application by providing access to data carriers and assistance when the Controller is required to take specific actions in connection with the exercise of the rights of the data subject.

(2) The deadline for reviewing the application and ruling on it shall be one month from receipt of the request. This period may be extended by a further two months, taking into account the complexity and number of requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, stating the reasons for the delay.

(3) The decision shall be communicated in writing to the applicant, received in person against signature or by post with return receipt. Where the data subject submits a request by electronic means, the information shall be provided by electronic means, unless the data subject has specified otherwise.

(4) Where the data do not exist or cannot be provided on a specific legal basis, the applicant shall be denied access to them by a reasoned decision. The refusal to grant access may be appealed by the person before the authority specified in the letter and within the specified time limit.

**Art.20**. The company shall publish the terms and conditions for exercising the rights of data subjects in accordance with the GDPR on its official website in the Rules for providing information on the exercise of the rights of personal data subjects.

## CHAPTER VI. RESPONSIBILITY AND CONTROL

**Art.21**.(1) Ongoing control over compliance with this Policy shall be exercised by the heads of the relevant units within the Company's structure (directorates/departments).

(2) Subsequent control of compliance with the requirements for lawful and fair processing of personal data shall be carried out by a specialized "Internal Control" service.

(3) At least once a year, the DPO shall inform the Board of Directors with a report on its activities, including the number and type of requests submitted for the exercise of the rights of data subjects, participation in procedures for the coordination of documents, DPIA, personal data security breaches, and, where necessary, propose specific measures in relation to compliance with the applicable personal data protection legislation.

(4) The Management Board shall periodically, but at least once a year, review this policy and the relevant internal documents that introduce rules, policies, and principles for the lawful and fair processing of personal data, updating them as necessary.

## FINAL PROVISIONS

**§1**. For the purposes of this Policy, the terms used shall have the meaning given to them by the GDPR and the Personal Data Protection Act.

**§2**. This policy shall be disclosed and made available to all employees of the Company through a shared resource on the internal corporate network for information and implementation.

**§3**. This Policy was adopted by the Management Board of Euroins on January 30, 2020, and enters into force on the same date, repealing the Instruction on the conditions and methods for the collection, processing, storage, and protection of personal data, adopted by a decision of the Company's Management Board on August 15, 2017. The policy was amended by a decision of the Company's Board

of Directors on December 18, 2020, and the changes are effective as of the same date. It was amended by a decision of the Board of Directors on December 10, 2025, and the changes are effective as of the same date.